Er du forberedt på cyberangreb i forsyningskæderne?

Kronik

Af adjunkt Peter Mayer, Institut for Matematik og Datalogi, SDU, lektor Marco Peressotti, Institut for Matematik og Datalogi, SDU samt professor Jan Stentoft, Institut for Erhverv og Bæredygtighed, SDU.

Med den stadigt stigende digitalisering af virksomheder bliver også forsyningskæderne mere digitaliserede. Denne digitalisering bringer fordele som fleksibilitet, men også ulemper som en øget trussel om cyberangreb.

Truslen om cyberangreb i forsyningskæderne giver stigende bekymringer for virksomheder af alle størrelser, men især for de små og mellemstore virksomheder (SMV'er). SMV'er har til sammenligning med store virksomheder færre finansielle og menneskelige ressourcer, og deres IT er ofte outsourcet til en ekstern leverandør, hvorigennem de er oplagte mål for hackere.

Angreb målrettes den software og de tjenester, som virksomhederne er afhængige af, og hackerne infiltrerer ofte SMV'erne gennem betroede leverandører og tredjepartsudbydere. Truslen for virksomhederne er tosidet. På den ene side kan virksomheder blive angrebet indefra gennem en såkaldt 'bagdør'. Det er en metode, der gennem software reelt set giver hackeren adgang til de systemer, han har lyst til.

Et sådant angreb kan standse driften og påføre SMV'erne store omkostninger, hvilket kan true deres eksistens. På den anden side kan virksomheder, der leverer digitale tjenester eller produkter til kunder, blive mål for cyberkriminelle, som forsøger at kompromittere disse ydelser for at infiltrere virksomhedens kunder.

En nylig begivenhed, der tydeliggør leverandørers indvirken på deres kunders systemer, er en hændelse hos cybersikkerhedsfirmaet CrowdStrike, som standsede driften af en lang række store og små virksomheder verden over. En forkert konfigureret opdatering fra CrowdStrike førte til utilsigtede systemnedbrud.

Selvom hændelsen ikke var forårsaget af et cyberangreb, men snarere af utilstrækkelige foranstaltninger af kvalitetskontrol, viste den, hvordan selv betroede leverandører kan forårsage nedbrud hos deres kunder.

Hackere er ofte villige til at investere meget tid og mange kræfter i cyberangreb, hvis de kan nå en bred vifte af virksomheder og data på én gang. Det kan de f.eks. ved at inficere et software, inden næste opdatering foreligger. Et eksempel er det såkaldte 'xz supply chain-angreb'.

Her brugte hackerne social engineering gennem tre år til at få kontrol over et open source-software, der bruges til at komprimere data og pakke filer i operativsystemet Linux.

Efter at have fået kontrol indsatte de en bagdør i det meget anvendte software. Først kort tid inden softwaren skulle udbredes til offentligheden, blev bagdøren opdaget, og cirkulationen blev forhindret.

I et andet eksempel fra 2020 lykkedes det hackere at indsætte en bagdør i det udbredte IT-system Orion fra virksomheden SolarWinds. Via koden, som softwarevirksomheden uden viden sendte ud til 18.000 kunder, heriblandt 150 danske virksomheder, fik hackerne adgang til følsomme data og systemer hos virksomhederne.

Hackerne gjorde meget for at skjule deres aktivitet og ventede på det rette øjeblik til at introducere bagdøren. Det understreger, hvor meget hackere er villige til at gøre, hvis nok virksomheder vil blive kompromitteret.

De førnævnte angreb fokuserede på via software at skabe bagdøre ind i digitale systemer. Andre cyberangreb sigter mod at forstyrre ikke-digitale forsyningskæder, som den målrettede SMV er en del af. Det har Leviathan, der er en gruppe af hackere forbundet med den kinesiske regering, praktiseret.

Gruppen gennemførte en række phishing-angreb, der specifikt rettede sig mod virksomheder i den maritime sektor, som leverede produkter til ikke-kinesiske udviklingsprojekter (f.eks. vindparker eller olieplatforme) i Det Sydkinesiske Hav.

Gennem cyberangreb forsøgte den kinesiske regering at forstyrre de maritime udviklingsprojekter i Det Sydkinesiske Hav, fordi de anså dem for at krænke Kinas krav som markeret i 'Nine-Dash-Line Kravet'. Mange leverandører i Europa var mål for disse angreb.

De ovennævnte eksempler er blot et udvalg af en bred vifte af forsyningskædeangreb, man som virksomhed kan blive ramt af. For at afværge cyberangreb, der trænger ind i virksomheden gennem betroede tredjepartsprodukter, er øget opmærksomhed på cyberangreb et vigtigt skridt.

Man kan f.eks. arbejde med at identificere kritiske IT-systemer og planlægge alternative leverandører af systemerne. Ved cyberangreb, der vil forstyrre virksomhedens digitale og ikke-digitale drift, er det afgørende at have en veldefineret beredskabsplan for at forsvare sig mod disse angreb.